OnDefend

Facilities Security Testing

Uncover Hidden Threats Across Your Facilities

Modern facilities are interconnected environments where physical infrastructure, networks, hardware, and human processes intersect, creating attack paths that no single-domain assessment can detect.

OnDefend facilities security testing assesses the full facility ecosystem across physical, digital, and human domains - uncovering exposure and control gaps in a single integrated assessment.

Testing Capabilities

Adversary-Driven Facilities Testing

Emulates adversaries across physical, technical, and human domains to identify realistic facility attack paths.

Physical Security & Access Control

Tests access controls, badge systems, and surveillance for weaknesses enabling unauthorized access and attack chaining.

Social Engineering & Human Risk

Tests phishing, pretexting, and physical social engineering to evaluate how human behavior bypasses controls.

Hardware & Embedded Systems Testing

Tests access control hardware, cameras, and controllers for firmware weaknesses and unauthorized communications.

Network & Infrastructure Testing

Assesses on-premises, hybrid, and cloud-connected facility networks for segmentation failures and lateral movement paths.

Cloud & Hybrid Facility Systems

Assesses cloud and hybrid platforms supporting facility operations for misconfigurations and cross-domain attack paths.

Outcomes

- Cross-domain attack paths identified across physical, network, hardware, and human domains
- Physical-to-digital attack paths validated with root cause analysis and remediation guidance
- Detection and response effectiveness measured across facility systems and incident response procedures
- Compliance support for physical security standards, validated against real adversary behavior

By testing facilities as integrated environments, organizations can uncover cross-domain risk and build resilience against adversaries operating across physical and digital domains.

OnDefend.com